REMARKS

These remarks follow the order of the paragraphs of the office action. Relevant portions of the office action are shown indented and italicized.

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless —

(b) the invention was patented or described in a printed publication in this or a foreign country or in public
use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 4-6, 13, 16, and 17 are rejected under 35 U.S.C. 102(b) as being anticipated by Brennan et al. (US Patent No. 5,675,649 and Brennan hereinafter).

In response, the applicant respectfully states that exception is taken with the equivalencies and anticipation of Claims 4-6, 13, 16, and 17 and .Brennan The claims are apparently not anticipated by .Brennan The present invention, claimed in Claims 4-6, 13, 16, and 17, [1-22] provides methods that:

"form the basis of a forward-secure signature scheme that is provably secure. Moreover, the presented methods form also the basis of a fine-grained forward-secure signature scheme that is secure and efficient. The scheme allows to react immediately on hacker break-ins such that signatures from the past still remain valid without re-issuing them and future signature values based on an exposed key can be identified accordingly. In general, each prepared signature carries an ascending index such that once an index is used, no lower index can be used to sign. Then, whenever an adversary breaks in, an honest signer can just announce the current index, e.g., by signing some special message with respect to

the current index, as part of the revocation message for the current time period. It is then understood that all signatures made in prior time periods as well as all signatures make in the revoked period up to the announced index are valid, i.e., non-reputable."

Thus, the claimed invention is directed to a forward-secure signature scheme that is provably secure, and that form the basis of a fine-grained forward-secure signature scheme that is secure and efficient. The scheme allows to react immediately on hacker break-ins such that signatures from the past still remain valid without re-issuing them and future signature values based on an exposed key can be identified accordingly.

The art to Brennan is entitled "Process for cryptographic key generation and safekeeping. The Brennan abstract reads:

> "A process for cryptographic key generation and safekeeping is provided. A plurality of key agents are selected, each having a copy of the source code. One copy of the source code is loaded onto a secure computer system and is compared with at least one other copy of the source code to validate the loaded copy of the source code. Master key information and locking key information are generated by executing compiled source code. The master key information is then separated into a plurality of master key shares which are distributed to master key agents such that each master key agent possesses one master key share. The locking key information is separated into a plurality of locking key shares which are distributed to locking key agents such that each locking key agent possesses one locking key share. Then, the plurality of locking key shares and the plurality of master key shares are validated, and the secure computer system is securely shut down."

Thus, Brennan is concerned with and directed to cryptographic key generation and safekeeping. Brennan is apparently not concerned with any forward-secure signature scheme that is provably secure, or a scheme that forms a basis of a fine-grained forward-secure signature scheme that is secure and efficient. Nor is Brennan apparently concerned with any scheme that allows reacting immediately on hacker break-ins such that signatures from the past still remain valid without re-issuing them and future signature values based on an exposed key can be identified accordingly. Thus, Claims 4-6, 13, 16, and 17 are not anticipated by Brennan and are allowable.

3. As to claim 4, Brennan teaches a method comprising providing a signature value on a message in a network of connected computer nodes, the method being executable by a first computer node and the step of providing comprising the steps of:

In response, the applicant respectfully states that exception is taken with the alleged teaching of claim 4 and claim element teaching or equivalencies stated in the office communication. Indeed, Brennan fails to teach

> *providing a signature value on a message in a network of connected computer nodes, or any concern with any method being executable by a first computer node*

The office communication continues:

> *selecting (i.e., adding) a first signature element (e.g., signature) (i.e., Brennan teaches adding a signature to certificate information [col. 12, lines 29-31]);*

Applicant respectfully states that exception is taken with the alleged teaching of any signature element, the signature is not a signature element but is rather the whole signature. Adding is not the same as selecting. Brennan col. 12, lines 29-31] has little relevance to any selection of a signature element.

> *selecting a signature exponent value from a number of exponent values (i.e., Brennan teaches (M must be a large integer which is the product of two large primes p and q. It is recommended that M have the same number of bit its binary expansion as does N. Absent specific knowledge ot p or q. M must be presumed computationally infeasible to factor [col. 10, lines 47-51]):*

Applicant respectfully states that exception is taken with the alleged teaching of claim 4 signature exponent value from a number of exponent values. Brennan col. 10, lines 47-51, does not anticipate any such value. Brennan alleged teaching of s (M must be a large integer which is the product of two large primes p and q. It is recommended that M have the same number of bit its binary has no relevance to any exponent vale or any signature exponent value from a number of exponent values.

> *expansion as does N. Absent specific knowledge of p or q. M must be presumed computationally infeasible to factor [col. 10, lines 47-51])*

Applicant respectfully states that exception is taken with the alleged teaching of claim 4 and Brennan. Brennan N, M. etc. are not an exponent value. Besides, any presumption that M must be presumed

computationally infeasible to factor [col. 10, lines 47-51] is not in claim 4.

> *and deriving a second signature element from a provided secret cryptographic key, the message, and the number of exponent values such that the first signature element, the second signature element, and the signature exponent value satisfy a known relationship with the message and a provided public cryptographic key, where the signature value comprises the first signature element, the second signature element, and a signature reference to the signature exponent value, the signature value being sendable within the network to a second computer node for verification (i.e., Brennan teaches a third stage comprises creation of a self-signed certificate attesting the certificate authority name, public module N, and public exponente and the validity period of these public key parameters. A secure hash function is applied to the certificate information to create a message digest, ext the message digest is encrypted with the certificate authority's secret key [col. 12, lines 22-30]).*

Applicant respectfully states that exception is taken with the alleged teaching of claim 4 and claim element teaching.

4. A method comprising providing a signature value on a message in a network of connected computer nodes, the method being executable by a first computer node and the step of providing comprising the steps of:

- selecting a first signature element from a plurality of signature elements comprising said signature;

- selecting a signature exponent value from a number of exponent values, said signature comprised of a plurality of signature exponent values; and

- deriving a second signature element from a provided secret cryptographic key, the message, and the number of exponent values such that the first signature element, the second signature element and the signature exponent value satisfy a known relationship with the message and a provided public cryptographic key, wherein the signature value comprises the first signature element, the second signature element, and a signature reference to the signature exponent value, the signature value being sendable within the network to a second computer node for verification.

Claim 4 is amended to make it more clear. However, Brennan does nothing and is not concerned with the step of deriving a second signature element from a provided secret cryptographic key, the message, and the number of exponent values such that the first signature element, the second signature element and the signature exponent value satisfy a known relationship with the message and a provided public cryptographic key, wherein the signature value comprises the first signature element, the second signature element, and a signature reference to the signature exponent value, the signature value being sendable within the network to a second computer node, in claim 4, in [col. 12, lines 22-30] or elsewhere. Thus, claim 4 and all claims of the present invention are not anticipated by Brennan.

4. As to claim 5, Brennan teaches a method where the step of deriving a second signature element (i.e., self-signed certificate) further comprises deriving a signature base value using a provided public cryptographic key, the provided secret cryptographic key, and the exponent values (i.e., Brennan teaches a creation of a self-signed certificate attesting to the certificate authority's name, public modulus N and public exponent e, and the validity period of these public key parameters. Brennan teaches a secure hash function is applied to the certificate information to create a message digest. Brennan teaches a next, the message digest is encrypted with the certificate authority's secret key, i.e. the message digest is signed by the certificate authority. Brennan teaches a signature is then added to the certificate information to complete the certificate [col. 12, lines 20— 32]).

5. As to claim 6, Brennan teaches a method further comprising deriving a new secret cryptographic key from the provided secret cryptographic key and the selected signature exponent value [col. 12,. lines 20— 32].

6. As to claim 13, Brennan teaches a method further comprising applying each of the exponent values to at most one signature value [col. 12, lines 20-32].

7. As to claim 16, Brennan teaches a computer program element comprising program code means for performing the method, when said program is run on a computer (i.e., Brennan teaches a computer used to execute source code to perform said functions [col. 4, lines 11-21]).

8. As to claim 17, Brennan teaches a computer program product stored on a computer usable medium, comprising computer readable program means for causing a computer to perform a method (i.e., Brennan teaches a computer used to

execute source code to perform said functions [col, 4, lines 11-21]),

Thus, claim 4 and all claims that depend on claim 4 and all claims of the present invention are not taught or anticipated by Brennan.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set
forth in section 102 of this title. ft the differences between the subject matter sought to be patented and
the prior art are such that the subject matter as a whole would have been obvious at the time the
invention was made to a person having ordinary skill in the art to which said subject matter pertains.
Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 USC. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CER 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

9. Claims 1, 9-12, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brennan in view of Murakami (US Patent Publication No. 2001/0010721).

In response, the applicant respectfully states that exception is taken with the equivalencies and anticipation of Claims 1, 9-12, and 22 and .Brennan with Murakami The claims are apparently not anticipated by .Brennan The present invention, claimed in Claims 1, 9-12, and 22 [1-22] provides methods that are directed to a forward-secure signature scheme that is provably secure, and that form the basis of a fine-grained forward-secure signature scheme that is secure and

efficient. The scheme allows to react immediately on hacker break-ins such that signatures from the past still remain valid without re-issuing them and future signature values based on an exposed key can be identified accordingly.

The art to Brennan is entitled "Process for cryptographic key generation and safekeeping. It was shown that Brennan is concerned with and directed to cryptographic key generation and safekeeping. Brennan is apparently not concerned with any forward-secure signature scheme that is provably secure, or a scheme that forms a basis of a fine-grained forward-secure signature scheme that is secure and efficient. Nor is Brennan apparently concerned with any scheme that allows reacting immediately on hacker break-ins such that signatures from the past still remain valid without re-issuing them and future signature values based on an exposed key can be identified accordingly.

The art to Murakami is entitled "Common key generating method, common key generating apparatus, encryption method, cryptographic communication method and cryptographic communication system. The Murakami abstract reads:

> When generating a common key for use in an encryption process of encrypting a plaintext into a ciphertext and a decryption process of decrypting the ciphertext into the plaintext, components which are contained in the secret keys of one entity and correspond to other entity as a communicating party are extracted and composition of all the extracted components is performed while shifting the components to generate a common key. Thus, the common key consisting of a larger number of bits than the number of bits in each of the extracted components is generated. A common key of any size is generated by adjusting the amount of shift.

Thus, Murakami is concerned with generating a common key for use in an encryption process of encrypting a plaintext into a ciphertext and a decryption process of decrypting the ciphertext into the plaintext. This is not useful in supporting the deficiencies of Brennan of anticipating or making the present claims obvious. Thus, Claims 1, 9-12, and 22 are not anticipated by Brennan and Murakami and are allowable.

> *10. As to claim 1, Brennan discloses a method comprising providing a secret cryptographic key and a public cryptographic key applicable in a network of connected computer nodes using a signature scheme, the method being executable by a first computer node and the step of providing comprising the*

steps of:

generating the secret cryptographic key by selecting two random factor values (e.g., M and x) (i.e., Brennan teaches a secret parameters M and x, once generated provided a means of producing a cryptographically secure source of random numbers Icol. 11, lines 60-63]),

multiplying the two selected random factor values to obtain a modulus value (i.e., Brennan teaches obtaining modulus value [N] [col.. 11, lines 64-671), and selecting a secret base value (i.e., desired modulus size) in dependence on the modulus value (col. 11, lines 64-67), where the secret base value forms part of the secret cryptographic key (i.e., Brennan teaches a secret exponent d for which is used in forming the secret key [cal. 12, lines 40-50];

generating the public cryptographic key by selecting a number of exponent values, and deriving a public base value from the exponent values and the secret base value (i.e., Brennan teaches a public key with exponent parameters [col. 12, lines 20-25]), where the public base value and the modulus value form part of the public cryptographic key (i.e., Brennan teaches a modulus and exponent value [col. 12, lines 20-25]);

and providing the public cryptographic key within the network; such that the public cryptographic key and at least one of the selected exponent values is usable for verifying a signature value (i.e., computationally infeasible) on a message to be sent within the network to a second computer node for verification (i.e., Brennan teaches M must be a large integer which is the product of two large primes p and q. It is recommended that M have the same number of bit its binary expansion as does N. Absent specific knowledge of p or q. M must be presumed computationally infeasible to factor [col. 10, lines 47-51]).

However Brennan does not expressly teach:

deleting the two random factor values;

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Brennan as introduced by Murakami. Murakami discloses:

deleting the two random factor values (to provide random value deletion capability [par. 50, lines 8-12]);

Therefore, given the teachings of Murakami, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Brennan by employing the well known features of random value deleting

disclosed above by Murakami, for which secure generation of cryptographic keys will be enhanced [par. 50, lines 8-121.

11. As to claim 9, Brennan teaches a method according to claim 1, further comprising applying each of the exponent values to at most one signature value [col. 12, lines 20-32].

12. As to claim 10, Brennan teaches a computer program element comprising program (i.e., source) code means for performing the method when said program is run on a computer (i.e., Brennan teaches a computer used to execute source code to perform said functions [col. 4, lines 11-21]).

13. As to claim 11, Brennan teaches a computer program product stored on a computer usable medium, comprising computer readable program means for causing a computer to perform the method (i.e., function) (i.e., Brennan teaches a computer used to execute source code to perform said functions [col. 4, lines 11-21]).

14. As to claim 12, Brennan teaches a network device (i.e., computer) comprising: a computer program product (i.e., code); a processor (i.e., computer) for executing the method; the processor (i.e., computer) having access to exchanged messages in the network (i.e., Brennan teaches a computer used to execute source code to perform said functions [cal. 4, lines 11-21]).

15. As to claim 22, Brennan teaches a computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing functions of a network device, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions (i.e., Brennan teaches a computer used to execute source code to perform said functions [col. 4, lines 11-21]).

Neither separately or in combination of Murakami and bran, there is no provision of methods or apparatus that are directed to a forward-secure signature scheme that is provably secure, and that form the basis of a fine-grained forward-secure signature scheme that is secure and efficient. The scheme allows to react immediately on hacker break-ins such that signatures from the past still remain valid without re-issuing them and future signature values based on an exposed key can be identified accordingly.

16. Claims 2 and 3 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Brennan in view of Murakami as applied to claim 1 above, and further in view of

Johnson (US Patent Publication No.2001/0014153).

17. As to claim 2 and 3 the system disclose by Brennan in view of Murakami teaches substantial features of the claim invention (discussed above) it fails to disclose:

> *A method further comprising providing a description of the exponent values within the network (claim 2).*

> *A method further comprising defining an order of the selected exponent values for enabling to communicate the validity of the signature value in the event of a detected intrusion (claim 3).*

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Brennan in view of Murakami as introduced by Johnson. Johnson discloses:

> *A method further comprising providing a description of the exponent values within the network (claim 2) (to provide exponent description capability within the network [par. 21, lines 10-1 41).*

> *A method further comprising defining an order of the selected exponent values for enabling to communicate the validity of the signature value in the event of a detected intrusion (claim 3) (to provide exponent order to prevent exposure attack [par. 30 — par. 34]).*

Therefore, given the teachings of Johnson, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Brennan in view of Murakami by employing the well known features of exponent description within a network disclosed above by Johnson, for which signature security will be enhanced [par. 21, lines 10-14].

18. Claims 7, 14, 18, and 19 are rejected under U.S.C. 103(a) as being unpatentable over Chaum (US Patent No. 4,996,711) in view of Brennan.

19. As to claim 7, Chaum teaches a method comprising verifying signature value

on a message in a network of connected computer nodes, the method being executable by a second computer node and the step of verifying comprising the steps of:

receiving the signature value from a first computer node (i.e., Chaum teaches a. receiving the signature value from a first computer node (This root is communicated to the second party's processor 1208 via a suitable communication link) [col. 20, lines 40-43); and;

and verifying whether the signature exponent value and part

of the signature value satisfy a known relationship with the message and a provided public cryptographic key, otherwise refusing the signature value, wherein the signature value was generated from a first signature element, a number of exponent values, a provided secret cryptographic key, and the message (i.e., Chaum teaches interval (the data processor means 1202 of a first party in conjunction with associated means 1204 is capable of determining an exponent from a first message using a procedure known to the first party and to a second party, the exponent containing at least one prime factor uniquely determined by the message. In addition, processor 1202 in conjunction with associated means 1206 is capable of forming a root on a constant known to both first and second parties, said root corresponding to the exponent. This root is communicated to the second party's processor 1208 via a suitable communication link (indicated by doffed lines in FIG. 12). Then processor 1208 in conjunction with associated means 1210 checks the received root by computing the exponent, raising the root to said exponent to produce a result and then verifying that the result is said constant) [col. 20, lines 31-46]).

However Chaum does not expressly teach:

deriving a signature exponent value from the signature value;

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Chaum as introduced by Brennan. Brennan discloses:

deriving a signature exponent value from the signature value (to provide exponent derivation capability [col. 11, lines 63-67]):

Therefore, given the teachings of Brennan, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Chaum by employing the well known features of exponent derivation disclosed above by Brennan, for which signature security will be enhanced [col. 11, lines 63-67].

20. As to claims 14, 18, and 19, the system disclose by Chaum teaches substantial features of the claim invention (discussed above) it fails to disclose.

A method further comprising applying each of the exponent values to at

most one signature value (claim 14).

A computer program element comprising program code means for

performing the method, when said program is run on a computer (claim 18).

A computer program product stored on a computer usable medium, comprising computer readable program means for causing a computer to perform a method (claim 19).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Chaum as introduced by Brennan. Brennan discloses:

A method further comprising applying each of the exponent values to at

most one signature value (claim 14) (to provide exponent value for said signature [col. 12, lines 20— 32]).

A computer program element comprising program code means for performing the method, when said program is run on a computer (claim 18) (to provide code means for performing a method when said program is run on a computer [col. 4, lines 11-21]).

A computer program product stored on a computer usable medium, comprising computer readable program means for causing a computer to perform a method (claim 19) (to provide computer readable program means for causing a computer to perform a method [col. 4, lines 11-21]).

Therefore, given the teachings of Brennan, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Chaum by employing the well known features of a computer readable

program means for causing a computer to perform a method disclosed above by Brennan, for which secure generation of cryptographic keys will be enhanced [col. 4, lines 11-21].

21. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Johnson in view of Staddon et al. (US Patent Publication No. 20040017916 and Staddon hereinafter).

22. As to claim 8, Johnson teaches a method comprising communicating within a network of connected computer nodes the validity of a signature value in the event of an exposure of a secret cryptographic key relating to the signature value, the step of communicating comprising the steps of:

defining an order of exponentvalues (par. 21, lines 1-10);

publishing a description of the exponent values and the order of the exponent values within the network (par. 21, lines 10-14):

the order of exponent values, and a provided public cryptographic key

(i.e, Johnson teaches a signature value comprising of a exponent, a key to determine validity of signature).

However Johnson does not expressly teach:

publishing a revocation reference to one of the exponent values

within the network such that the validity of the signature value is determinable by using the revocation reference

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Johnson as introduced by Staddon. Staddon discloses:

publishing a revocation reference (i.e., revoke user are made public) to one of the exponent values within the network such that the validity of the signature value is determinable by using the revocation reference (to provide revocation notification of revoked parameters Ipar. 117, lines 4-8]).

Therefore, given the teachings of Staddon, a person having ordinary skill in the art at the time of the invention wQuld have recognized the desirability and advantage of

modifying Johnson by employing the well known features of revocation notification disclosed above by Staddon, for which signature validation will be enhanced par. 117, lines 4-8].

23. Claims 15, 20, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Johnson in view of Staddon as applied to claim 8 above, and further in view of Brennan.

24. As to claims 15, 20, and 21, the system disclose by Johnson in view of Staddon teaches substantial features of the claim invention (discussed above) it fails to disclose.

A method further comprising applying each of the exponent values to at most one signature value (claim 15).

A computer program element comprising program code means for performing the method, when said program is run on a computer (claim 20).

A computer program product stored on a computer usable medium, comprising computer readable program means for causing a computer to perform a method (claim 21).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Johnson in view of Staddon as introduced by Brennan. Brennan discloses:

A method further comprising applying each of the exponent values to at most one signature value (claim 15) (to provide exponent value for said signature [col. 12, lines 20— 32]).

A computer program element comprising program code means for performing the method, when said program is run on a computer (claim 20)

(to provide code means for performing a method when said program is run on a computer [col. 4, lines 11-21]).

A computer program product stored on a computer usable medium, comprising computer readable program means for causing a computer to perform a method (claim 21) (to provide computer readable program means for causing a computer to perform a method [col. 4, lines 11-21]).

Therefore, given the teachings of Brennan, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Johnson in view of Staddon by employing the well known features of a computer readable *program means for causing a computer to perform a method disclosed above by Brennan, for which secure generation of cryptographic keys will be enhanced [col. 4, lines 11-21].*

Neither separately or in combination of Murakami, Johnson, Johnson, Staddon and/or bran, there is no provision of methods or apparatus that are directed to a forward-secure signature scheme that is provably secure, and that form the basis of a fine-grained forward-secure signature scheme that is secure and efficient. The scheme allows to react immediately on hacker break-ins such that signatures from the past still remain valid without re-issuing them and future signature values based on an exposed key can be identified accordingly. Thus all claims 1-22 are allowable over all the combined cited art.

It is anticipated that this amendment brings claims 1-21 to allowance. If any questions remain, please contact the undersigned representative before issuing a FINAL action.

Please charge any fee necessary to enter this paper to deposit account 50-0510.

Respectfully submitted,

By: ___/Louis Herzberg/_____
Louis P. Herzberg
Reg. No. 41,500
Voice Tel. (845) 352-3194
Fax. (845) 352-3194

3 Cloverdale Lane
Monsey, NY 10952

Customer Number: 54856